习题课 14

1 (i) $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$

(ii) $\dim(\mathrm{Im}(\varphi))=3$

$\dim(\ker(\varphi))=4-\dim(\mathrm{Im}(\varphi))=1$

(iii) $\varphi(\bar v)=\begin{pmatrix} \bar 4 \\ \bar 2 \\ \bar 2 \end{pmatrix}=\begin{pmatrix} \bar 0 \\ \bar 0 \\ \bar 0 \end{pmatrix}$ (给出最终结果)

(以上矩阵运算均在 $\mathbb{Z}_2$ 中)

2.

证明：由于 $\bar A\cdot\bar A^{adj}\equiv|\bar A|\cdot\bar E_n \pmod 5$

故 A 可逆 $\pmod 5$ $\Longleftrightarrow$ $\det A\not\equiv 0 \pmod 5$

$\det\bar A=\bar 1\neq\bar 0$，故 A 可逆.

计算 A^{-1}：

$$\left(\begin{array}{ccc|ccc} \bar 1 & \bar 0 & \bar 2 & \bar 1 & & \\ \bar 0 & \bar 3 & \bar 0 & & \bar 1 & \\ \bar 2 & \bar 0 & \bar 1 & & & \bar 1 \end{array}\right) \xrightarrow{-2(1)+(3)} \left(\begin{array}{ccc|ccc} \bar 1 & \bar 0 & \bar 2 & \bar 1 & & \\ \bar 0 & \bar 3 & \bar 0 & & \bar 1 & \\ \bar 0 & \bar 0 & \bar 2 & \bar 3 & & \bar 1 \end{array}\right)$$

$$\xrightarrow{-(3)+(1)} \left(\begin{array}{ccc|ccc} \bar 1 & \bar 0 & \bar 0 & \bar 3 & \bar 0 & \bar 4 \\ \bar 0 & \bar 3 & \bar 0 & \bar 0 & \bar 1 & \bar 0 \\ \bar 0 & \bar 0 & \bar 2 & \bar 3 & \bar 0 & \bar 1 \end{array}\right) \xrightarrow[(2)\times 2]{(3)\times 3} \begin{pmatrix} \bar 3 & \bar 0 & \bar 4 \\ \bar 0 & \bar 2 & \bar 0 \\ \bar 4 & \bar 0 & \bar 3 \end{pmatrix}$$

3 $\begin{cases} x_1+2x_2+x_3+2x_4=1 \\ x_1+x_3=2 \\ x_1+x_2+x_3+x_4=0 \end{cases}$ 在 $\mathbb{Z}_3$ 中解的个数

解：

$$M=\left(\begin{array}{cccc|c} 1 & 2 & 1 & 2 & 1 \\ 1 & 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

($x_1+x_2=2$ 可得的解集为 $\{(u,v,2-u,1-v)^T \mid u,v\in\mathbb{Z}_3\}$

$\begin{cases} x_1+x_3=2 \\ x_2+x_4=1 \end{cases}$ 方程的解集为 $\{(u, v, 2-u, 1-v)^T \mid u, v \in \mathbb{Z}_3\}$

故共有9个解.

4. (i) 证明：① $\bar{m}=0$ 时，$\bar{m}^p=0$，命题成立

② $\bar{m}\neq 0$ 时，$\bar{m}\in \mathbb{Z}_p^*$，由 Lagrange 定理

$(\bar{m})^{p-1}=\bar{1}$，故 $(\bar{m})^p=\bar{m}$

(ii) 对 k 作归纳

$k=0$ 时 显然

$k=1$ 时，见 ln14 命题4.9

假设 $k-1$ 时命题成立，对 k 的情形

$(\bar{a}+\bar{b})^{p^k}=\left((\bar{a}+\bar{b})^{p^{k-1}}\right)^p=\left(\bar{a}^{p^{k-1}}+\bar{b}^{p^{k-1}}\right)^p=\bar{a}^{p^k}+\bar{b}^{p^k}$.

故命题对 k 的情形成立.

5 证明有限整环是域

证明：设 D 为有限整环，$\forall a\in D$，$a\neq 0$，令

$f: D\to D$
$d\to ad$

若 $f(d_1)=f(d_2)$，$ad_1=ad_2$
$a(d_1-d_2)=0$ D为整环，$a\neq 0$
故 $d_1=d_2$，f单，又D有限，故f满

$\Longrightarrow \exists\, d\in D$，$ad=e$，故D为域.

6. 设F是域，$A\in M_n(F)$ 且 $A\neq 0$.

(i) 设 $B\in F[A]$ 且 $B\neq 0$. 证明：B是环F[A]的零因子 $\Longleftrightarrow$ $\operatorname{rank} B<n$

(ii) 设 $C\in M_n(F)$. 证明 $\operatorname{rank}(C)<n \Longleftrightarrow \exists M\in M_n(F)$，$M\neq 0$ 满足

$MC=CM=0$

证明：(回顾 ln14 例3.20，ln10 命题9.4)

(i) 必要性：若 $\exists\, C\neq 0$ $BC=CB=0$，且 $\operatorname{rank} B=n$，则 B^{-1} 存在

$C=B^{-1}BC=0$ 矛盾，故 $\operatorname{rank} B<n$

充分性：若 $\operatorname{rank} B<n$，设 $f(x)\in F[x]$ 为次数最小的满足 $f(B)=0$

的多项式，$f(x)=a_0+a_1x+\cdots+a_mx^m$，由于 $f(B)=0$，故 $a_0=0$

$f(B)=a_1B+a_2B^2+\cdots+a_mB^m=0$，$B(a_1+\cdots+a_mB^{m-1})=0$

由 f 次数极小性，$a_1+\cdots+a_mB^{m-1}\neq 0$.

由于 $B\in F[A]$，$a_1+\cdots+a_mB^{m-1}\in F[A]$，这说明 B为F[A]零因子.

由于次数极小性，$a_1+\cdots+a_m B^{\cdots} \neq 0$.
由于 $B\in F[A]$，$a_1+\cdots+a_m B^{m-1}\in F[A]$，这说明 B 为 $F[A]$ 零因子.
（本题一个很直观的想法是 $\text{rank}B<n \Longrightarrow Bx=0$ 存在非0解
将其扩充成一个矩阵 C，$BC=0$，但难说明 $C\in F[A]$）.

(ii) 证明与(i)类似
（充分性是显然的，关于必要性，另一个做法如下：
由于 $\text{rank}(C)<n$，故 $Cx=0$ 存在非0解 α，$y^TC=0$ 存在非0解 β，
则 $\alpha\beta^T\in M_n(F)$，$C\alpha\beta^T=\alpha\beta^TC=0$ 且 $\alpha\beta^T\neq 0$.）

补充

1. 简单的有限域（元素个数有限的域）

① $\mathbb{Z}_p$ 为 p 元有限域

② $\mathbb{Z}_3(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}_3\}$ 为 9 元有限域

③ $\mathbb{Z}_2(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in\mathbb{Z}_2\}$ 不是有限域（有零因子）

2、设 G 为幺半群，s.t $\forall a,b\in G$，$ax=b$，$ya=b$ 有唯一解，
则 G 为群
证明：幺半群 $\longrightarrow$ 群，我们需证明 $\forall x\in G$，x 有逆元.
仍以 a 为例. 设 $a\in G$，$\exists\, x_a,y_a\in G$，s.t $ax_a=e=y_a\cdot a$
则 $x_a=ex_a=y_a\cdot ax_a=y_a\cdot e=y_a$，故 $x_a=y_a=a^{-1}\in G$，
G 为群

3 将 2 中 G 改为半群，其余条件不变，证明 G 为群.
证明：在 2 基础上，只需说明 G 有幺元 e.
设 $\forall a,b\in G$，$\exists\, x,y_e\in G$，$y_e a=a$，$ax=b$
则 $y_e b=y_e ax=ax=b$，由 b 任意性，可设 y_e 为左幺元
设 $\forall a,b\in G$，$\exists\, y,x_e\in G$，$ax_e=a$，$ya=b$
则 $bx_e=yax_e=ya=b$，同理可设 x_e 为右幺元.
$x_e=x_e y_e=y_e$，故 $x_e=y_e$ 为幺元.

4. 设 G 为一非空有限集，其中定义了乘法 ab（对乘法封闭），且

4. 设 G 为一非空有限集，其中定义了乘法 ab（对乘法封闭），且

(i) $a(bc)=(ab)c$

(ii) $ab=ac \Rightarrow b=c$

(iii) $ac=bc \Rightarrow a=b$　　证明 G 为群

证明：① $\forall a_1 \in G$，$a_1 G = G$，$\Rightarrow \exists\ a_e \in G$，$a_1 a_e = a_1$，

$a_1 a_e \cdot a_1 a_e = a_1^2$

$a_1 a_e \cdot a_1 = a_1^2$

$a_e \cdot a_1 = a_1 = a_1 \cdot a_e$

对 $\forall a_i \in G$，$a_i \cdot a_e \cdot a_1 = a_i \cdot a_1 \Rightarrow a_i \cdot a_e = a_i$，$a_e$ 为右幺

同理可知 ∃左幺 a_e'，则 $a_e' = a_e' \cdot a_e = a_e$，故幺元存在，记为 e.

② 对 $\forall a_i \in G$，$\exists\ a_i', a_i''$ s.t $a_i \cdot a_i' = a_i'' \cdot a_i = e$

则 $a_i' = a_i' \cdot e = a_i' \cdot a_i \cdot a_i' \Rightarrow a_i' \cdot a_i = e = a_i'' \cdot a_i$

$\Rightarrow a_i' = a_i''$ 即为 a_i^{-1}，故逆元存在.

5. 令 $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$，$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$，$K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

$$H = \{ a + bI + cJ + dK \mid a, b, c, d \in R \}$$

(i) 证明 H 是环

(ii) 证明 H 不是域

（证明可由以下事实得出：$I^2 = J^2 = K^2 = -E$，

$IJ = K = -JI$，$JK = I = -KJ$，$KI = J = -IK$）

（进一步，H 为含幺环，至少含有 2 个元素，且全体非 0 元对乘法成一群，这种结构称为体，这是一个很反常规的代数结构）

6. 设 $A \in M_n(R)$ 满足 $A^2 = A$，求证：∃ n 阶方阵 P s.t

$$P^{-1}AP = \begin{vmatrix} E_r & 0 \\ 0 & 0 \end{vmatrix}, \quad r = \text{rank} A.$$

证明：见习题课 12. 例 1.